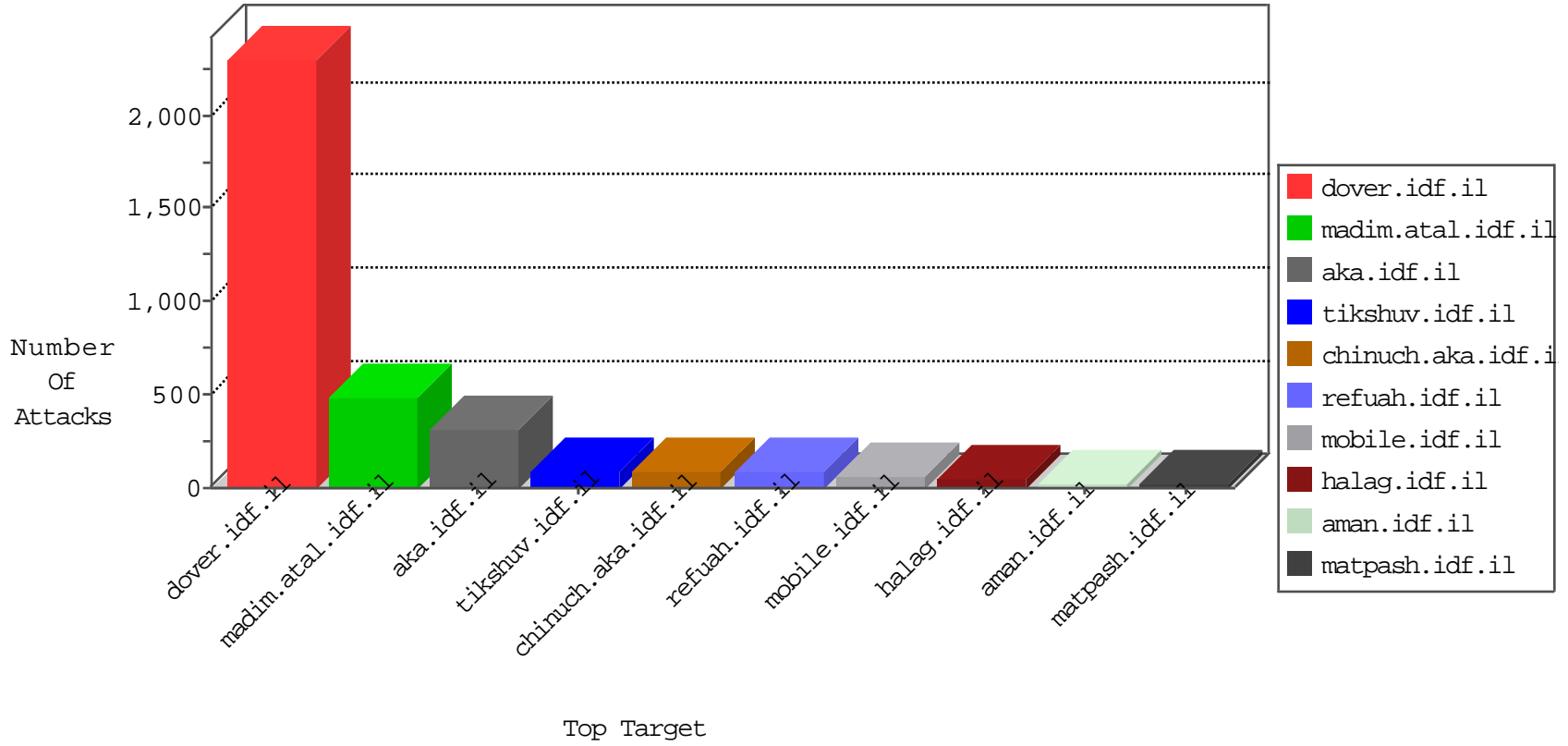


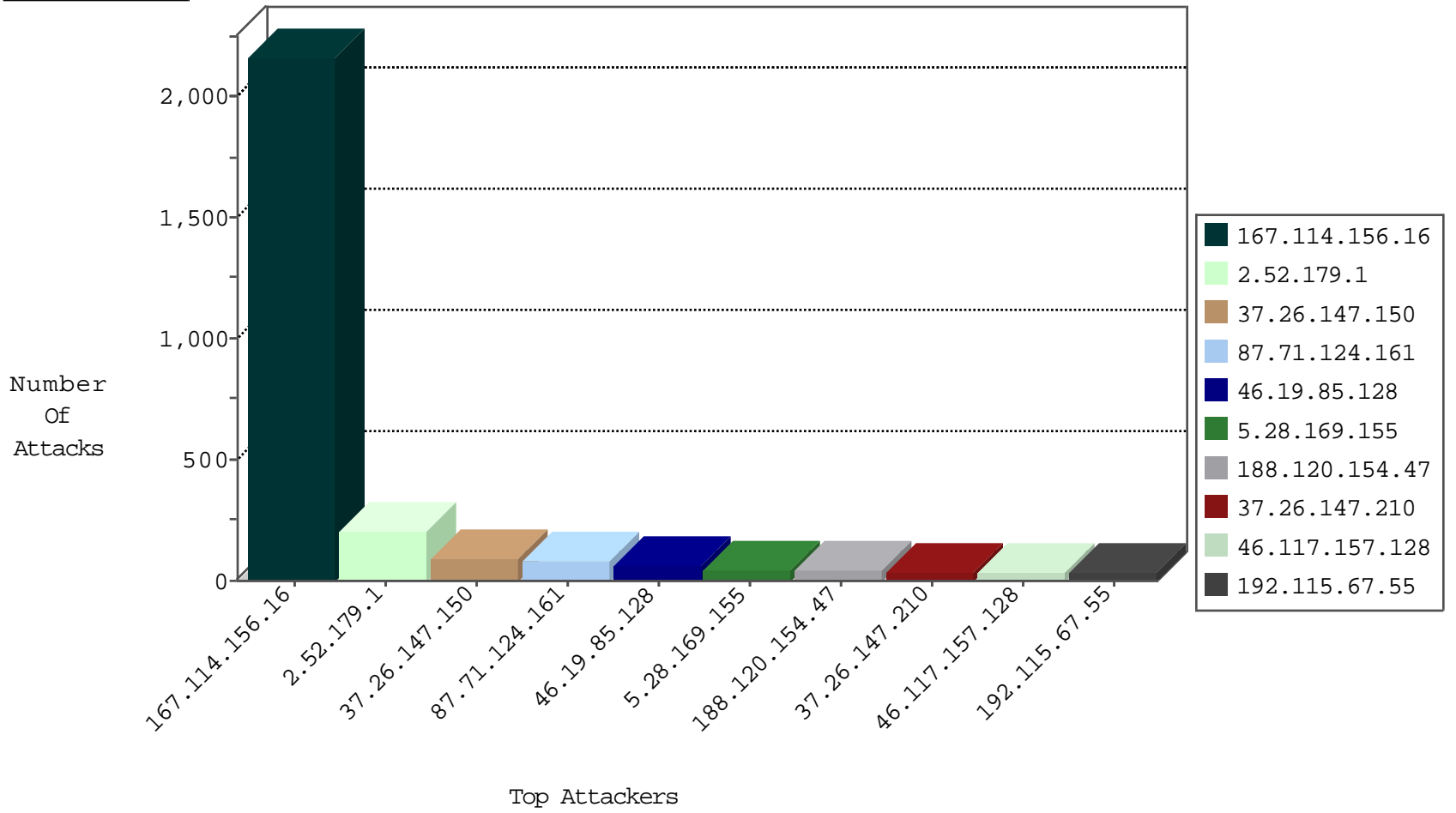
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3404
168.235.197.20	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.197.20	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
185.120.126.10		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.115.67.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	30
79.181.71.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
89.163.148.58	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
89.163.148.58	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
89.163.148.58	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.7.107	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	2
89.163.148.58	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
89.163.148.58	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
89.163.148.58	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
91.121.221.15	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.137	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.197.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.202.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
97.82.188.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.7.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.136.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.192.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.213.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
71.177.22.76	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
71.177.22.76	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.97.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.73.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.129.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.242.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.167.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.170.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
71.177.22.76	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.71.124.161	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	73
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	44
5.28.169.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
188.120.154.47	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.117.157.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
109.253.129.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.86.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.32.179.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
176.13.16.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.157.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
109.64.42.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.166.65.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.70.81.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
149.78.79.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.130.240.165	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.3.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
80.178.195.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.9.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.218.209	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.203.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.0.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.16.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.235.85.235	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
185.120.126.122		147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
176.13.16.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
168.235.197.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.154.22.110	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.235.85.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.240.165	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
192.118.68.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.4.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.21.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.71.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.240.165	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.175.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.178.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.66.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.169.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

03-13-2016-12:04:07 to 03-13-2016-13:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.134.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.59		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.179.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	206
37.26.147.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
37.26.147.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
213.57.240.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.26.146.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
80.246.140.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.6.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
65.54.247.156	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.54.247.156	Block	3
109.253.130.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
95.35.186.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.135.187	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1684	Block	3
37.26.149.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.138.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.177.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
31.154.25.50	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
93.172.173.43	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
2.54.2.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.251.250	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.85.63	Israel	147.237.76.31	nakchal.idf.il	Distributed Unknown HTTP Request Method	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
37.26.147.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/menu-ending.gif	Block	1
5.28.169.155	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Abnormally Long Request method	Block	1
94.230.93.214	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.179.230.18	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspxaman	Block	1
82.166.65.237	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.239.70.113	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
176.13.9.34	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
79.179.111.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/doctrine/doctrine.stm"	Block	1
2.54.188.245	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
93.172.173.43	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 93.172.173.43	Block	1
80.246.139.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/faq.asp	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in URL	Block	1
94.230.93.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.54.247.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx/webresource.axd	Block	1
213.8.7.156	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.89.217.235		147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/./images/shared/youtubenew.png	Block	1
85.250.50.103	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
37.26.146.209	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1